Google Play Protect

Fortnite Task Force

Privileged & Confidential

Status: Draft
Created: 2018-08-06
Author: Lydia Ash [redacted]@google.com), Jason Woloz [redacted]@google.com), William Luh [redacted]@google.com)
Shortlink: go/fortnite-tf

Issue du jour: go/hijacking-fortnite-installs and the larger problem detailed here
Epic Games: https://issuetracker.google.com/112630336. This is currently restricted to Android team members and Epic Games. I sent a report (pointing them to the bug) to Security Bugs (Epic) , and they have acknowledged.

Samsung: https://partnerissuetracker.corp.google.com/112632028

Metrics:

- Metrics for harmful and unwanted app infection rate (from jehuang@): go/fortnite-metrics
- Chrome warnings from imposter sites

OBJECTIVE

To ***quantify*** and ***protect*** users who install Fortnite (unknown sources required for installation) or a fake MUwS fortnite.

ROADMAP FORWARD - 8/20pm

- ***Next Sync:*** *we are likely cancelling the daily sync going forward - will be confirmed Monday and deleted/notified at that time*
- ***Epic*** - Bug filed
  - Ed flipped the bug public just before 10am MTV time
  - Shannon has tipped off Android Central and the Security reporter at Wired. Things are moving slowly (it's a Friday in August...). Android Central article will likely go today or over the weekend and then we forecast this will get picked up more on Monday.
  - The article went live during the sync - https://www.androidcentral.com/epic-games-first-fortnite-installer-allowed-hackers-download-install-silently
- ***Samsung*** - bug filed
  - ***PREVIOUS AI: DaveK*** to check with security team as to if the Samsung problem is no

EXHIBIT 122

longer a vulnerability. If Samsung is still a vulnerability, then we need to follow up with ***Jamie/Purnima*** on potentially flagging the Samsung installer.
    - ***PREVIOUS AI: Purnima*** to talk with Jamie should we ask Samsung if there are other installers similar to this?
    - ***NEXT AI:*** Waiting on mid-Sept for Samsung's push.
- ***Installers*** - Review anything that purports to be an installer Review for other mild attacks (FN and Orange).
    - Ed and Purnima discussed BD contacts for the markets.
    - Ed: The info is included in this doc, and you can see an example of the bug I would be filing (that will eventually become public) there.
      The app stores in question are:
      9Apps: largest 3P app store (India, Brazil, Russia, Indonesia), owned by Alibaba.
      Cafe Bazaar: main app store in Iran, and 2nd largest 3P store worldwide.
      Aptoide: a somewhat popular 3P app store, also a complainant in various EU cases (+cc Michael FYI).
    - ***AI: Ed*** to link the bugs in this doc
- ***GPP*** - Decide how to harden GPP. Messaging is "GPP is getting more aggressive, and it will be felt if you do not do certain "good behavior" Android policy things.
    - go/off-market-enforcement
    - DaveK: Talked to Hiroshi today. He was OK on the general concept and asked that William continue to work on a specific proposal (we will tune the one in the go link and gather input from all here). In addition, he suggested we should consider even more out-of-box ideas on this. For example, we talked about the possibility of Pixel/Foo not allowing untrustworthy unknown sources at all (e.g. there could be a whitelist of approved non-Play sources that meet certain security requirements). His words in follow up after our meeting:
        - *Yes I think we should explore all kinds of options here to make it clear to our users when they are doing something insecure. Maybe we need to go further than "making it clear" and it requires us to rethink our stance. So I think it's worth brainstorming various ideas and exploring pros and cons.*

      Legal opinion on guidelines here will obviously be critical...
- ***Public coverage***
    - Repeat from above Epic section
        - Shannon has tipped off Android Central and the Security reporter at Wired. Things are moving slowly (it's a Friday in August...). Android Central article will likely go today or over the weekend and then we forecast this will get picked up more on Monday.
        - The article went live during the sync - https://www.androidcentral.com/epic-games-first-fortnite-installer-allowed-hackers-download-install-silently
    - Reactive PR is prepped for further inquiries. No further outreach will be done.
    - ***AI: Shannon*** to continue to monitor.
- ***Legal***

Redacted - Privilege

Redacted - Privilege

- ***Going forward*** - the immediate fires are handled and we do not appear to need the daily sync going forward. However given the difficulty in getting time on cal and the possibility for something to still blow up in the press this meeting will stay on calendar temporarily. We anticipate the daily sync being cancelled, but will make that determination Monday afternoon based on latest information.
  We will continue to monitor the Samsung side of this and the GPP policy and determine any followup conversations or meetings from that.
  - ***AI: ALL*** to weigh in if we need to keep daily standups or to come back together again.

- ***William*** / Android Security team needs to spot check a few of the surfaces of the app to ensure there are no other changes we need to have addressed.
  - b/112583938: We have a few volunteers from Android Security
  - Ed's doc has been LGTM'ed by a few in Android Security (see bug) and also some in Android Security are going to see if there are other vulnerabilities
- ***Ed*** will poke around at the Fortnight installer a bit more - can we get somebody else on R&D team to verify this, too?? DaveK will get Salvador or Sebastian to do this.

Edward Cunningham (Google) **Comment [1]:** Ed, could you file a bug describing the verification that is needed and link it here? We'll take a look.

Comment [2]: Filed here: https://b.corp.google.com/issues/112583938

- GPP Business Analytics team working on building dashboards so everyone can track the current Fortnite malware infection rate

WEEK END SUMMARY 2018-08-10

- Unknown sources enabled on ~39% of ecosystem (stats from jehuang@)
- Fortnite imposter apps/sites: collected, collected, collected (driven by jwoloz@)
- Dashboard for Fortnite imposter on Play setup: go/trackdbi
- DaveK sync with execs about off-market enforcement
  - Proposal for off-market enforcement started: go/off-market-enforcement
- Sync with SafeBrowsing team and filed a bug to create dashboard/graphs to track efforts at flagging fake Fortnite sites
- YouTube Scaled Abuse (see 2018-08-09)

OPEN ACTION ITEMS

Team	***Action Item***	***Bug / status (in lieu)***

Reporting / Risk Assessment [BA doc]		
Jenny	Track how many devices have Fortnite and impersonated Fortnite installed (blocked by R&D and MUwS teams) break down by PHA vs MUwS, Play vs. Off-market	b/112286227
Jenny	Track how many devices with Fortnite installed that didn't have unknown source setting on prior	b/112467981
Anand	Provide Ad-clicks and payout related metrics	b/112560861

Anand Thudukuchi Ramanathan
Comment [3]: + (Google)
Assigned to Anand Thudukuchi Ramanathan

Comment [1]: Hi Anand, please feel free to provide the link to your metrics here. Thanks!

Find all the counterfeits, PHA and MUWs		
Jason	Marlo - Detect Counterfeit Fornite Submissions	b/112268992
Jason	Fortnite copycat tracking	go/trackdbi
William/Dave	Proposal for off market enforcement	go/off-market-enforcement (not widely shared yet)
William and pstanton@	Make sure that Safebrowsing warns users about Fortnite impersonation sites.	b/112350117
Kylie	Fortnite Off-market Web Distribution Collab. is here	https://colab.corp.google.com/drive/1cMSb3PX_nV32TRmxNyU_uKUBoDdlf30g
R&D + MUWS Ops	Investigate fake Fortnite apps and come up with a way to flag new fake Fortnite apps as MUwS Track detected Fortnite imposter apps found offmarket, submitted to Play review (unpub); detected on Play using a "fortnite-imposter" label unuchek@ to collaborate with mtt@ on MUWOps to see if Fortnite impersonation apps like these are also PHA and flag when detected PUBG sweep	b/112270795 - in progress b/112342262 - in progress
Eng bugs		
CS	Make sure MUwS field is passed back to BA tables	b/112284878 - in progress
Jenny	Work with R&D and SB to generate tables (daily refreshed) of confirmed PHA and muws/impersonation for scaled tracking	https://b.corp.google.com/issues/112270795#comment27 https://b.corp.google.com/issues/112342262#comment13
Wei Jin	Whitelisting to avoid automation/human to flag any apps from the cert	b/112555139
T&I	Figure out how to get more storage	b/72052582

Take down Fakes from Google services and Partners		
William/Rahul	Take down fake Fortnite advertised on YT pages	See meeting notes 2018-08-09
Jason	Track Fake Fortnite ads	Exec escalation b/112560861
Jason	Reach out to Facebook and give them a heads-up. We already talk to FB as part of PHA referrals so this could be tied in there.	See meeting notes 2018-08-13 b/112439939
Sentiment and Social Media		
Tiff	Tracking sentiment of Fortnite	Sentiment analysis

Suggestions from DaveK's email:
Since Epic CEO has publicly stated they take their security responsibility very seriously, we could recommend they take some additional precautions to help protect users, e.g.:

1. App can check if GPP is enabled and refuse to run if it isn't (encouraging users who continue to sideload to be better protected)

2. App can check for unknown sources being enabled and require the user to disable them before the game is played (the user would then re enable temporarily if the app needs an update)

3. App can use SafetyNet attestation to ensure the device has good integrity (I think they already do this?)

4. App should target recent OS (v26+), following Play best practices

We could also consider a blog that explains all this to developers. About 45% of devices currently

Comment [5]: I think this is a great suggestion.

Comment [6]: +1, but I wonder if they intend to target China market where almost all phones have this enabled.

Comment [7]: They already do this it turns out: https://screenshot.googleplex.com/67Dedh8MM3g.png

Comment [8]: Yes, they have integrated the API and are requesting additional quota. There is a thread discussing this, as I had suggested that we might not want to grant them quota. This comes at a big cost to Google (just like Pokemon Go, real SWE hours will be used fighting abuse on their behalf), so we need to be thoughtful about whether we really want to sign up for this for a big non-Play app. Ends up being in part a business decision.

Comment [9]: I would recommend that they use the VerifyApps API instead - I know they're not the same, but they would help with concerns that we have

MEETING NOTES

ATTENDEES
jeffreyjo@, jchuang, kylicm@, pstanton@, sauravc@, williamluh@

MEETING NOTES

- Dashboards for PHA/MUwS and Safe Browsing/Chrome hit are linked at the very top of the doc under metrics
- jchuang@ went over PHA/MUwS dashboard, and it looks like the infection rate is negligible
- pstanton@ went over click rate to sites to fake Fortnite sites and these are also negligible

    - Note that Google can only track Chrome and not WebView
    - William to reach out to facebook to see if they have additional data
- saurav@ says there have been 0 ads that try to promote fake Fortnite APKs in the past week
- Talked about other games, like GTA, and decided we should wait to see how Fortnite pans out before we invest any effort into other games.
- kyliem@ mentioned we should document what we learnt from Fortnite tracking and also what can we re-use for future investigations like this - a lot of the work here requires manual reviewing so it was deemed difficult to ever fully automate

ATTENDEES

Core task force: Colin Smith, Lydia Ash, Shannon Newberry, Mike Hochberg, Tian Lim, Purnima Kochikar, Tristan Ostrowski

MEETING NOTES

- ***Epic*** - Bug filed
    - Ed flipped the bug public just before 10am MTV time
    - Shannon has tipped off Android Central and the Security reporter at Wired. Things are moving slowly (it's a Friday in August...). Android Central article will likely go today or over the weekend and then we forecast this will get picked up more on Monday.
    - The article went live during the sync - https://www.androidcentral.com/epic-games-first-fortnite-installer-allowed-hackers-download-install-silently
- ***Samsung*** - bug filed
    - ***PREVIOUS AI: DaveK*** to check with security team as to if the Samsung problem is no longer a vulnerability. If Samsung is still a vulnerability, then we need to follow up with ***Jamie/Purnima*** on potentially flagging the Samsung installer.
    - ***PREVIOUS AI: Purnima*** to talk with Jamie should we ask Samsung if there are other installers similar to this?
    - ***NEXT AI:*** Waiting on mid-Sept for Samsung's push.
- ***Installers*** - Review anything that purports to be an installer Review for other mitd attacks (FN and Orange).
    - Ed and Purnima discussed BD contacts for the markets.
    - Ed: The info is included in this doc, and you can see an example of the bug I would be filing (that will eventually become public) there.
      The app stores in question are:
      9Apps: largest 3P app store (India, Brazil, Russia, Indonesia), owned by Alibaba.
      Cafe Bazaar: main app store in Iran, and 2nd largest 3P store worldwide.
      Aptoide: a somewhat popular 3P app store, also a complainant in various EU cases (+cc Michael FYI).
    - ***AI: Ed*** to link the bugs in this doc
- ***GPP*** - Decide how to harden GPP. Messaging is "GPP is getting more aggressive, and it will be

felt if you do not do certain "good behavior" Android policy things.
    - go/off-market-enforcement
    - DaveK: Talked to Hiroshi today. He was OK on the general concept and asked that William continue to work on a specific proposal (we will tune the one in the go link and gather input from all here). In addition, he suggested we should consider even more out-of-box ideas on this. For example, we talked about the possibility of Pixel/Foo not allowing untrustworthy unknown sources at all (e.g. there could be a whitelist of approved non-Play sources that meet certain security requirements). His words in follow up after our meeting:
        - *Yes I think we should explore all kinds of options here to make it clear to our users when they are doing something insecure. Maybe we need to go further than "making it clear" and it requires us to rethink our stance. So I think it's worth brainstorming various ideas and exploring pros and cons.*

      Legal opinion on guidelines here will obviously be critical...
- ***Public coverage***
    - Repeat from above Epic section
        - Shannon has tipped off Android Central and the Security reporter at Wired. Things are moving slowly (it's a Friday in August...). Android Central article will likely go today or over the weekend and then we forecast this will get picked up more on Monday.
        - The article went live during the sync - https://www.androidcentral.com/epic-games-first-fortnite-installer-allowed-hackers-download-install-silently
    - Reactive PR is prepped for further inquiries. No further outreach will be done.
    - ***AI: Shannon*** to continue to monitor.
- ***Legal***

Redacted - Privilege

- ***Going forward*** - the immediate fires are handled and we do not appear to need the daily sync going forward. However given the difficulty in getting time on cal and the possibility for something to still blow up in the press this meeting will stay on calendar temporarily. We anticipate the daily sync being cancelled, but will make that determination Monday afternoon based on latest information.
  We will continue to monitor the Samsung side of this and the GPP policy and determine any followup conversations or meetings from that.
    - ***AI: ALL*** to weigh in if we need to keep daily standups or to come back together again.
    -

ATTENDEES

Core task force: Colin Smith, Lydia Ash, Shannon Newberry, Ed Cunningham, Mike Hochberg, Tian Lim

MEETING NOTES

- ***Epic*** - Bug filed
  - Shannon did the research with Ed and agreed to do either 7 or 14 days to public release - that would put it at going public either 8/24 or 8/31
  - We could flip the bug Fri morning (8/24) and then point 3 friendlies at it, but not release any new metrics or data points. Could also have Lookout point to some other potential malware scams as a separate article and align to when the bug goes public - working on this with Lookout. We would likely need to feed that number to Lookout - DaveK is already on that thread. There is a small chance that Samsung could catch some bad press as it does specifically call out Samsung devices.
  - ***Question: Mike and Tian*** - are you good with pointing reporters at the bug? And to wait 14 days to do the flip to make it public? And ok with using Lookout to put out malware stat?
  - Not sure we trust Lookout to put the message out there exactly as we want. Not sure Lookout will position that we're earning out 30% - it could add more fuel to it.
  - Could let Lookout put their piece out there and eval the reaction.
  - ***DECIDED: Ed*** to flip the bug on 8/24 at early morning LON time (just past the precise 8/23 4:12pm 7 day extension), then ***Shannon*** can tip people off on Fri 8am if nobody has picked it up organically.
  -
- ***Samsung*** - bug filed
  - ***UPDATE*** Samsung has provided additional perspective in the bug this morning
  - Ed: Essentially their writeup says that Samsung will make some changes to update the verifier in mid-Sept.
  - ***PREVIOUS AI: DaveK*** to check with security team as to if the Samsung problem is no longer a vulnerability. If Samsung is still a vulnerability, then we need to follow up with ***Jamie/Purnima*** on potentially flagging the Samsung installer.
  - ***PREVIOUS AI: Purnima*** to talk with Jamie should we ask Samsung if there are other installers similar to this?
  - ***NEXT AI:*** Waiting on mid-Sept for Samsung's push.
- ***Installers*** - Review anything that purports to be an installer Review for other mitd attacks (FN and Orange).
  - Ed: We have other installers with issues - Indian app store and Iranian - so far we've found 3 of the largest third party app markets: 9 apps, apptoied, cafe bazaar. The apps they download could be switched at the last minute. It's an identical vulnerability.
  - Bugs will be filed on Friday about these situations and vulnerabilities
  - Are they copying open source code? Or is it coincidence that they are all making the same mistake? They appear to all be taking a path of least resistance which is creating a similar pattern. The mitd writeup faults Google for giving people the tools to do this.

Should change the way installers work in Q with storage.
    - ***AI: Ed*** to work with ***Purnima*** about any BD contacts for these.
    - ***AI: Ed*** is logging bugs on these now and will link them in this doc.
- ***GPP*** - Decide how to harden GPP. Messaging is "GPP is getting more aggressive, and it will be felt if you do not do certain "good behavior" Android policy things.
    - ***PREVIOUS AI: DaveK*** to talk with Hiroshi. Proposal is stable. go/off-market-enforcement
    - ***PREVIOUS AI: William*** (and DaveK) to reach out to TT for perspective
- ***Public coverage***
    - Reactive PR is ready to go.
      "User security is our top priority, and as part of our proactive monitoring for malware we identified a vulnerability in the Fortnite installer. We immediately notified Epic Games and they fixed the issue." - Google spokesperson
- ***Legal***

Redacted - Privilege

ATTENDEES

Core task force: Colin Smith, Lydia Ash, Tristan Ostrowski, Mike Hochberg, Tian Lim, Shannon Newberry

MEETING NOTES

- ***Epic*** - Bug filed
    - Tristan checked in with Kristin (legal counsel). We give 7-14 days to get the message out, but we don't wait longer "just because".
    - We need Ed's info from Project Zero.
    - Purnima and Mike checked in and are concluding on 2 weeks.
    - Shannon talked with Ed this morning and Ed said 7 days was fine.
    - ***AI: Shannon*** to circle back with Ed and confirm 7 days. Shannon and Colin will determine the date the bug would go public.
- ***Samsung*** - bug filed
    - ***PREVIOUS NEXT AI:*** Hold waiting on more from Samsung
    - ***PREVIOUS AI: DaveK*** to check with security team as to if the Samsung problem is no longer a vulnerability. If Samsung is still a vulnerability, then we need to follow up with ***Jamie/Purnima*** on potentially flagging the Samsung installer.
    - ***PREVIOUS AI: Purnima*** to talk with Jamie should we ask Samsung if there are other installers similar to this?
- ***Installers*** - Review anything that purports to be an installer Review for other mitd attacks (FN and Orange).
- ***GPP*** - Decide how to harden GPP. Messaging is "GPP is getting more aggressive, and it will be

felt if you do not do certain "good behavior" Android policy things.
    - ***PREVIOUS AI: DaveK*** to talk with Hiroshi. Proposal is stable. go/off-market-enforcement
    - ***PREVIOUS AI: William*** (and DaveK) to reach out to TT for perspective
- ***Public coverage***
    - ***AI: Colin and Shannon*** is polishing up the statements and strategy for PR and press. PR is ready to go by the time the bug goes public.
- ***Legal***

Redacted - Privilege

ATTENDEES

Core task force: Colin Smith, Lydia Ash, Tristan Ostrowski, Mike Hochberg, Tian Lim

MEETING NOTES

- ***Epic*** - Bug filed
    - Epic pushed a fix 8/16 at 1pm; Ed verified and shared on thread this was validated
    - Epic requested (on bug) the full 90 days before sharing publicly
    - Tristan shared that we have the flex to wait the full 90 days, but we are not required to
    - Will 90 days delay put users at risk?
    - ***AI: Ed*** is looking in to this with Project Zero as to if we can or should wait 90 days
    - We should mark the old versions of the Epic app as PHA. The disclosure of the bug will help with the mark of PHA for the app.
    - In terms of setting precedent for future situations, we should play out a few other scenarios to ensure we have solid principles. If Fortnight refused to patch, we would flag for PHA. Lots of examples of apps which were found to be vulnerable and then flagged as PHA, most were ones that came in through Play.
    - The bug that was filed for Epic mentions Samsung...a bit messy....
    - Should we be flagging the Samsung Installer, too? In terms of a purist process, this would seem to be the course of action.

    - ***AI: DaveK*** to check with security team as to if the Samsung problem is no longer a vulnerability. If Samsung is still a vulnerability, then we need to follow up with ***Jamie/Purnima*** on potentially flagging the Samsung installer.
    - ***AI: Colin*** to grab somebody from DaveK's team (***Jason***) to get examples prepped for PR.
    - ***PENDING DECISION:*** Get Ed's guidance from Project Zero. Coordinate the timing of the bug release and flagging as PHA.
- ***Samsung*** - bug filed
    - ***PREVIOUS NEXT AI:*** Hold waiting on more from Samsung
    - ***PREVIOUS AI: Purnima***: should we ask Samsung if there are other installers similar to this?
    - Samsung seems to think that with Epic having made their patch, they do not need to do anything. There's some back and forth in the thread.
    - See AI above - DaveK to follow up with security team to verify if more needs to be done.
- ***Installers*** - Review anything that purports to be an installer Review for other mitd attacks (FN and Orange).
- ***GPP*** - Decide how to harden GPP. Messaging is "GPP is getting more aggressive, and it will be felt if you do not do certain "good behavior" Android policy things.
    - DaveK plans to talk with Hiroshi on Tuesday. It's stable and no changes since Tuesday. go/off-market-enforcement
    - ***PREVIOUS AI: William*** (and DaveK) to reach out to TT for perspective
- ***Public coverage***
    - Gathered edits to the statement.
    - Need to decide when we flip the Epic bug.
    - ***AI: Colin*** to also ask Jason of other examples where we've publicized using Buganizer.
    - ***AI: Colin*** is polishing up the statements and strategy for PR and press. PR is ready to go by Tuesday.

ATTENDEES

Core task force: Mike Hochberg, Colin Smith, Lydia Ash

MEETING NOTES

- ***Epic*** - Bug filed
    - ***UPDATE: Epic***: *We are currently testing a fix that will resolve this issue on all supported versions of Android (Down to API 19). Once internal testing is complete, we will roll this out to users via our self-update mechanism. Barring any last minute bugs or deployment blockers, we hope to get this out by late tonight or sometime tomorrow. If there are any changes to this tentative timeline, we will let you know.*
    - Anticipating they will flip the bug 6pm on Fri (8/17)
    - Concerns that they have stipulated that they will fix on newer phones, and we're not sure what they are planning to do as a fix
    - ***AI: Ed*** to monitor the bug and validate that Epic's fix is effective (should we validate on

both "newer" and "older" versions?)

- ***Samsung*** - bug filed
  - ***UPDATE***: ED: *still unclear if Samsung considers their own API flawed or not*
  - ***NEXT AI:*** Hold waiting on more from Samsung
  - ***AI: Purnima***: should we ask Samsung if there are other installers similar to this?
- ***Installers*** - Review anything that purports to be an installer Review for other mild attacks (FN and Orange). Do a sweep of anything that purports to be an installer.
  - ***UPDATE***: ***Ed Update***: *I began looking into this today. The only other app that obviously includes code to use the Galaxy Apps InstallAgent API was the Orange Updater - however in my testing it appears the app isn't currently whitelisted by Samsung (so can't use the API successfully). Not sure what the situation is there. I think we should ask Samsung who else they permit to use the API.*
    For other installers that are vulnerable to the Man-in-the-Disk vulnerability, we need to discuss our approach with the GPP R&D team. I did a quick check of two popular stores today and found both are vulnerable (see screen recordings for 9Apps and Aptoide where I inject the fake Fortnite app). I've little doubt that many others are in the same position.
    The other big one with relevance to Samsung I began taking a look at today is Facebook App Manager. I don't have anything to report right now, but it definitely does make use of external storage for its downloads so seems worth a closer look.
- ***GPP*** - Decide how to harden GPP. Messaging is "GPP is getting more aggressive, and it will be felt if you do not do certain "good behavior" Android policy things.
  - ***PREVIOUS AI: DaveK*** is planning to gather feedback and then take for Hiroshi - go/off-market-enforcement
  - ***PREVIOUS AI: William*** (and DaveK) to reach out to TT for perspective
- ***Public coverage***
  - Now in the news - Wired article
  - Colin is working on a reactive statement, will link in these notes for distribution when task force notes go out
  - ***AI: Colin*** to link drafts for statements and distributions before Lydia sends meeting notes
  - ***AI: Colin*** to reach out to Jason Woloz and Shie about installs of fake Fortnight apps in last 14 days, how many we remove from Play store, etc
- **Redacted - Privilege**

Attendees

Core task force: Colin Smith, Lydia Ash, Tristan Ostrowski, William Luh, Purnima Kochikar, Mike, Tian Lim

RAW MEETING NOTES

- ***Epic*** - Bug filed. outreach to them.

    - Purnima sent mail to Mark Rian who immediately responded to escalate internally.
    - Epic did respond on the bug early today.
    - Next AI: Waiting on Epic
- ***Samsung*** - bug filed. notified of bug.
    - Jamie sent out email, it's national holiday
    - Next AI: Waiting on Samsung
- ***Installers*** - Review anything that purports to be an installer Review for other mitd attacks (FN and Orange). Do a sweep of anything that purports to be an installer.
    - ***AI: William*** following up with Ed on this to see if we can get somebody on security team to verify there aren't other similar situations
- ***GPP*** - Decide how to harden GPP. Messaging is "GPP is getting more aggressive, and it will be felt if you do not do certain "good behavior" Android policy things.
    - 2 fronts
        - Proposal for off-market enforcement started: go/off-market-enforcement
            - This is not agreed on yet - need Hiroshi to review
            - Need comms to properly communicate once we make a decision
            - ***AI: DaveK*** is planning to gather feedback and then take for Hiroshi
        - This is an issue and will be for a long time (possibly 90 days). Concerns this leaves a vulnerability for a long time.
            - Do we need a new process for OEMs to have a shorter window to fix?
            - ***DECISION:*** No. We will stay with the standard 90 days.
            - Maybe this is actually a question as to if the Samsung store is behaving as a PHA and we should be flagging them?
            - ***AI: William*** (and DaveK) to reach out to TT for perspective
- ***Public coverage*** - anything of note? point friendlies at bug once public
    - Nothing is public at the moment, no coverage
    - ***AI: Colin*** is prepping a reactive blog strategy and the proper whispers when bugs do get made public
- ***AI: Lydia*** to have someone review TGIF dory for any questions about this

Attendees

jwoloz@, pstanton@, andrewahn@, jeffreyjo@, jehuang@, sauravc@

- Jenny presented graph for number of installs of MUwS and PHA fortnites
- MUwS: looking for icons
- Marlo: Is the app confusing users and making them think it's the real fortnite?
- Safe Browsing: Sites the refer/redirct users to these PHAs
    - Track warnings that are shown to users (dashboard linked)

    - Track search demoted
    - 30 sites
- Adwords: Bug created for Maurice - Saurav will follow up. Also Ads enforcement summary on T&S Ads side.
- Play: Track increasing trend whether more bad fortnites coming in - Andrew to sync with Jenny on who to work with to track this.

Attendees

Jamie Rosenberg, Purnima Kochikar, Colin Smith, Tian Lim, Lydia Ash, Sameer Samat, Tristan Ostrowski; group then talked with Hiroshi to verify pathway forward

RAW MEETING NOTES

- Purnima - Met with Ed this morning, figured out the process on filing the bug, verified with Tristan; We still need to figure out if we send it to Epic to their publicly available security reports, or do we use Bill on Purnima's team to inform Epic - either way this starts the clock for 15 days before public disclosure. Our connection at Epic is Mark Ryan (cofounder and commercial partnerships), and we also work with their head of studio.
- Jamie: We should give Mark the FYI about the security bug.
- Tian: Epic has already updated their installer, but not sure on what changed
- ***AI: Ed:*** To re-verify the installer before we go back to Epic
- Do we have other mitd attacks? Unknown and this was basically an attack that was announced that day. Our position is
- ***AI: Ed:*** Review for other mitd attacks (FN and Orange). Do a sweep of anything that purports to be an installer.
- ***AI: Purnima:*** Through BD contact, we should make sure all managed partners who have installers (FB, Orange, carriers, etc) are informed that we will be doing a sweep and scan.
- ***AI: Purnima:*** To follow up with Jason Woloz to get the security sweep across installers
- ***AI: Colin:*** Once the bug goes public, we'll point friendlies at it and they can do their own coverage
- Jamie: KR Independence day starts today our time for them. Holiday there
- ***AI: Tian*** to check in with Ed in the morning on anything late breaking and known
- FOLLOWUP VERIFICATION WITH HIROSHI
    - Plan we reviewed
        - File a bug that is not immediately public with Epic, give 15 days to fix after which the bug goes public after they either fix the bug or the 15 days elapsed. *[In Play for a similar situation, we would give 7 days window]*
        - Purnima team give Epic a call letting them know about the bug.
        - Steering: Do not call it Project Zero. File a private bug in the Android bug tracker and not through Project Zero, point Epic at this.

Comment [10]: + Paul Stanton (Google) Hi Paul, do you think you will be able to get a dashboard for this by the next meeting? If so please share the dashboard with everyone and add it at the top where it says metrics so all the execs are able to access them. Thanks! _Assigned to Paul Stanton_

Comment [11]: I have a table that shows how many warnings we've shown in Chrome at safebrowsing_ops_dremel.fortnite_chrome_warnings . + Jenny Huang (Google) would you like to include that in your dashboard so we can minimize number of dashboards?

Comment [12]: To avoid potential misinterpretation on data, I'd suggest we all create our own dashboard. It would be great if you can share the link to your dashboard here. Thanks Paul!

Comment [13]: Dashboard is now linked, please let me know if there are issues viewing it. This does not take into account any Search demotions, someone in Webspam or T&S Search would know how to pull that data if available. One other note is this is only for Chrome, we don't have figures for Webview which may be more of a primary driver of these apps (links out from twitter, messaging, facebook. etc.).

Comment [14]: Saurav Chakraborty (Google) _Assigned to Saurav Chakraborty_

Comment [15]: https://buganizer.corp.google.com/issues/112560861

Comment [16]: Play: Track increasing trend whether more bad fortnites coming in - Andrew to sync with Jenny on who to work with to track this. + Andrew Ahn (Google) _Assigned to Andrew Ahn_

Comment [17]: Per most recent guidance this has now change to be 90 days.

        - For Samsung, use existing buganizer channel, and on a path to go public after 15 days if not fixed.
        - Colin can then point reporters to the two bugs as they become public.
    - H: Make it so!
- ***DECIDED***: We need to file one bug with Epic and a different bug with Samsung. We need to prep both bugs today and get them ready - the Samsung bug should be filed on the Samsung/Google channel. These should be coordinated to be filed at the same time, but not the end of the world for Samsung to be filed tomorrow. File the bug with Epic today. Simultaneously have Purnima's team reach out to Mark to let him know we have filed the bug. ***Purnima is coordinating the bug prep, entry, and outreach to each Samsung and Epic.*** The core task force will reconvene tomorrow afternoon. We can at least make progress as a core group and send notes to update Sameer and Jamie. If a subsequent call is needed in the evening, we can set that up.

Attendees

Jamie Rosenberg, Purnima Kochikar, Colin Smith, Tian Lim, Mike Hochberg, Dave Kleidermacher, Lydia Ash, Sameer Samat, Ed Cunningham, William Luh, Tristan Ostrowski

RAW MEETING NOTES

- When we file the bug report for Project Zero, the bug will be the first thing that Samsung or Epic would see from us. This would then start the 15 day clock before it goes public.
- ***For Samsung***: Jamie will cover with ES when they connect, tell him we're filing the bug in private repository that is shared with Samsung. We won't coach them on how to make it better, but just make them aware of the issue we've seen in the installer. Setting an aggressive timeline of 15 days to fix. Wording "After 15 days elapsed, or a fix is available, we will disclose publicly."
- ***For Epic***: We need to take Ed's bug write up and translate into a conversation with the partner. ***Lydia*** will first talk with ***Purnima*** to get a partner writeup.
- ***AI:*** Next 24 hours is our chance to identify if there's a third or fourth issue that we want solved with this. GPP team needs to spot check a few of the surfaces of the app to ensure there are no other changes we need to have addressed. GPP team to dig in to
- ***DECIDED***: Take next 24 hours to polish up communication plan to Epic. By EOD Tuesday, we should be communicating with both Epic and Samsung
- ***NEXT STEPS:*** No communication tonight. We get H's take tomorrow morning and then communicate with both Epic and Samsung tomorrow (Tues).
- **Redacted - Privilege**
- ***Ed*** will reach out to EMEA's Zero team to ensure our steps for navigating the bug logging and potential public buganizer component creation are set correctly.

Comment [18]: + William Luh (Google)
Assigned to William Luh

Comment [19]: + Salvador Mandujano (Google)
Sebastian Porst (Google)

Can someone from R&D team please take a look at Ed's doc:

Comment [20]: go/hijacking-fortnite-installs and peer review it and also see if we can see if there are other vulnerabilities.

Comment [21]: Is the goal here to find other vulns in Fortnite or other apps with the same vuln?

Comment [22]: I believe the goal is to identify other problems specific to Fortnight or to Samsung, not the same problem exploited by other apps, so that if we press for a fix from Epic it is complete and thorough. William can correct me if I'm off here, though

Comment [23]: We're not really vulnerability researchers on our team. Wondering if someone else wants to pick this up.
+ Chad Brubaker (Google) + Zach Riggle (Google) + Ivan Lozano (Google)

Comment [24]: Yes that is correct. Android Security in general lost it's "Attack" team more than a year ago, so if we can verify Ed's work that is probably all that we can ask for.

Comment [25]: + Vishwath Mohan (Google) + Dan Austin (Google)

Comment [26]: + Billy Lau (Google)

FYI the doc describing the vuln is here:

go/hijacking-fortnite-installs

Comment [27]: The main need is for a quick sanity check of the findings by someone. Of secondary importance is figuring out if there are other similar issues in the Fortnite Installer to report (I would not be surprised at all if there are others).

Comment [28]: Per Salvador Mandujano (Google) above, I filed https://b.corp.google.com/issues/112583938 to track this.

Comment [29]: I wouldn't mind helping with this, sounds interesting.

Comment [30]: Thanks!

Comment [31]: Thanks, Ivan.

- ***Ed*** will poke around at the Fortnight installer a bit more - can we get somebody else on R&D team to verify this, too?? DaveK will get Salvadore or Sebastian to do this.
- Will use Hiroshi leads meeting at 9:30 to get his steer. We need to meet later tomorrow to get clarity on steps for execution.
- ***Tristan*** will give Kent a heads up after the Hiroshi meeting.

Attendees

Jamie Rosenberg, Purnima Kochikar, Colin Smith, Tian Lim, Mike Hochberg, Dave Kleidermacher, Lydia Ash, Sameer Samat, Ed Cunningham, , Tristan Ostrowski

RAW MEETING NOTES

- Fortnight's dist strategy has created a vulnerability
- Related to Samsung, PR strategy, Ads strategy (unless it's malware, we're going to sell ads for it)
- Need to get the word out on PR side, even as we're working to fix it
- This is essentially a "man-in-the-disk" vulnerability that we had identified in theory but had not seen an exploit
- If Checkpoint had discovered this initially, they would usually have gone directly to the developer to fix before publishing
- "We've found a vulnerability, it's changing the way we treat this internally, and we're going to address it immediately."
- We need to contact Samsung quickly and tell them about it to get it fixed
- It's not hard for Epic to fix this issue - they should have it fixed within 90 days
- Samsung could have provided better APK verification when the APK is passed to it - mostly this is a Fortnight issue, but the Samsung installer has whitelisted it
    - The installation really is a two part issue - it's a Fortnight problem as well as a Samsung problem - Fortnight downloads to a public storage space, and Samsung has a whitelist that can easily be spoofed
- Samsung should be doing an actual signature check
- PR strategy
    - DaveK: Users are at risk in several ways, many copycats, it's just a mess; somebody (Google?) should be telling the world how bad this is. Can we say it? Or will Epic just refuse to work with us?
- Sameer: Question is what we want to do, pulling back a bit - Ultimately we want Samsung to stop this kind of stuff (enabling the FN installer), we want other developers to realize this is complicated and there's a lot of ways to mess up, and as a result of those 2 we want FN to feel the pressure and make fixes, and we want the world to know that this is not safe to do this. We need to make it safe and have an aggressive future action for GPP. We need to lay down a case for the reasons why we have to do this. On Samsung - what is the best way to make them feel a tremendous amount of heat?
- JamieK: I should hear back from ES this afternoon, his team is looking into it. A chance he may conclude that they think this is stupid and they should not be doing this - 50/50 chance. If they don't, then we need to tell them about this and the additional vulnerabilities they are enabling.

- Sameer: We need to decide how much we want to escalate as a Hiroshi/DJ conversation - sort of us telling them "Now you're just creating vulnerabilities and we're both going to end up losing."
- When a user is installing, they need to go through unknown sources
- So how do we resolve Samsung's request for foldables help with this security vulnerability? If nothing else, this creates a massive distraction to their foldable requests.
- Sameer: Disclose just the Samsung vulnerability to Samsung if ES comes back to Jamie saying he can't do anything, and at that point Hiroshi talks with DJ. Separately we need to decide how to disclose the Epic thing to Epic and to Samsung.
- Sameer: Then laying out the case for doing something aggressive in GPP to address this - there's something which disrupts the app if a bunch of conditions are not met - and is there anything we can tighten up on unknown sources as well? We need to lay out this case. Lookout is a part of this as they have identified a bunch of vulnerabilities, disclosing the Epic bug is a part. Maybe we don't give a 90 day window to fix, we should start with 15 days.
- ***AI***: Decide how to harden GPP. Messaging is "GPP is getting more aggressive, and it will be felt if you do not do certain "good behavior" Android policy things.
- ***AI***: Need to make an official security advisory contact to Samsung and Epic - and this needs to be coordinated with Jamie's conversation with Samsung. Coordinate the conversation between partner and security as outreach. Samsung tact: You shouldn't be doing this, you don't have the virus scanning and security apparatus to do this, and on top of that you're highly permissive on how this can be installed which is not how we have our APIs and checks.
- ***AI***: Determine if our peer-to-peer sharing downloader is a version of the Samsung problem. What are our differentiators that make this safe so that we can push consistently on Samsung that we don't have a back door. It does feel awkwardly close to what Samsung is doing.
- ***DECIDED***: Epic needs to use internal storage.
- ***DECIDED***: Samsung needs to not do this with their installer API and not expose themselves to this handoff.
- ***TO DO***: Ed/DaveK - work on script about how we explain to Samsung what their problem is without going to too much detail. Separately a script about how we explain to Epic. We should give them 15 days to fix.
- ***TO DO***: Take a closer look at P2P before it launches (Mike and Tian)
    - William Luh is looking at this, too
    - GPP (William) following up with TL (Matt Patterson) for frosting team to verify P2P checks for sharing installing - will follow up with Mike:
        - According to mapatt@ copied to secure storage and the frosting metadata includes the digest of the APK, and the entire metadata is signed by Play and then verified by Play store prior to installation

Objective: Samsung SD card install API vulnerability

Attendees: dkleidermacher@, williamluh@

The following proposal was discussed and approved by dkleidermacher@, ssamat@, and other execs and conveyed in this meeting to assign action items:

1. TLDR: ejc@ found out that Samsung was helping Fortnite get installed without having to enable unknown sources; their approach was to have Fortnite app downloaded onto the SD card, call a Samsung store API that then installs the Fortnite app from the SD card, thus bypassing unknown sources - the problem is that this is vulnerable to malware replacing the Fortnite app with a malicious version and having Samsung blindly install the malware
2. Proposal is to write up two bugs saying that Google is going to flag Samsung app store and Fortnite app in 15 days if this continues, and then share these bugs separately with each company respectively - bug should outline vulnerability and possibly some suggestions
3. On day 15, regardless of whether Samsung or Fortnite has taken action, a blog post will be published outlining this vulnerability and furthermore hinting that we will be creating a new policy to enforce large user-base off-market apps (go/off-market-enforcement - execs were receptive to this proposal) in the future (this will be a separate blog)
4. AI 1: Reach out to ejc@ who is composing the two separate bugs as part of Point #2
5. ~~AI 2: Reach out to lydiaa@ to help *deploy* these two bugs to the two companies - by *deploy* we mean reach out to someone in Samsung and in Epic with a link to the bug and appropriate text~~ AI 2: Jaime has reached out to Samsung already and asked them to fix the problem, so waiting on Samsung to reply.
6. AI 3: Reach out to ejc@ to see if he is interested in authoring the blog post (Point #3)
7. AI 4: Reach out to jehuang@ to see if it's possible to get better stats on infection rate for the blog in Point #3.
8. AI 5: Inform GPP team of the possibility of flagging these two apps if after 15 days the vulnerability has not been addressed

Comment [32]: Jenny Huang (Google)
Assigned to Jenny Huang

AI: Send out nightly progress emails to include everything that happened that day.

Objective: Facebook Fortnite abuse vector

Attendees: skaram@, maryliz@, jeffreyjo@, andrewahn@, williamluh@

- Facebook already has a system for detecting malware, phishing, adware, but it is not very mature and they are already working with Google through skaram@ to see if both companies can share information to help both our detection systems work better
- AI (completed): Reach out to Facebook and ask them to use the Safe Browsing API, which will help detect fake Fortnite sites as well as fake Fortnite ads

Objective: YouTube Scaled Abuse and Fortnite policies

Attendees: laurelbrown@, witekr@, rafarodriguez@, rahmis@, williamluh@

- The Scaled Abuse team is already on this problem: they are working with the SafeBrowsing tema to scan all URLs
  - Embedded URLs in video and description will be scanned: ETA end of Q3 to mid Q4
  - URLs in comments, live chat will be scanned next year
  - Burned in URLs (non-clickable images in the video) can also be scanned, but technology is too good at extracting and lots of false positives
  - Mostly automated except for burned in URLs, which will require human review
- Fortnite traffic on youtube ranks well due to popularity of the keywords.
- Current scam appears to be for getting free vbucks. The Video is typically taken down.
- Upcoming launch next week is to are to start looking at the content / links outside of the video (using keywords and not Safe Browsing)
- Content will be taken down based on the policy that this is driving traffic offsite.
- This automated system is going to start next week with porn (using keywords and not Safe Browsing)

Objective: GPP team sync

Attendeeds: DaveK, Jason, Sebastian, Jenny, William

Quantify

- Jenny found 45% (updated to ~39% after we found O+ devices were being included incorrectly) of devices have unknown sources turned on
- Decided that we should track how many real and fake fortnite apps are installed on devices
- Salvador's team to work with mtt@ to mark fake Fortnite apps as MUwS
- William's team to ensure this info gets propagated back to BA tables
- Also suggested that we can track how many devices turned on unknown sources explicitly to install Fortnite (real or fake), and whether they get more PHAs thereafter

Protect

- Can we reach out to Epic and have them enforce that unknown sources is turned off, and that GPP is enabled? See DaveK's email for more info.

DOCUMENT HISTORY

For living documents, you may want to keep a history of significant revisions. When you add a significant new revision to the document, add a new line to the table below.

Date	*Author*	*Description*	*Reviewed by*
2018-08-06	williamluh	First meeting	